AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Leland W. Blank, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

1. I am a detective for the Kansas City, Missouri Police Department ("KCPD") and a Task Force Officer ("TFO") for the Federal Bureau of Investigations ("FBI"). As a Detective for the KCPD I investigated violent crimes for approximately 13 years, I received training about interviewing and interrogation, utilizing social media and phone data in investigations, and various other topics. As a TFO with the FBI, I investigate criminal related computer intrusion matters involving botnets, darkweb markets, malicious software, the theft of personal identification information, and other computer-based fraud. Since joining the FBI Cyber Task Force, I have been involved in several criminal investigations involving computer intrusions. I have received training in computer technology and computer-based fraud.

2. I am one of the officers principally responsible for the FBI investigation of Shawn Burkhalter, a/k/a "Deuce" ("Burkhalter") and Joshua Nesbitt, a/k/a "T," ("Nesbitt") that resulted in the Second Superseding Indictment in Case No. 18-00036-01/02-CR-W-BCW in this district. The Second Superseding Indictment (D.E. 816) charges Burkhalter and Nesbitt with the following violations of federal law: illegal drug distribution conspiracy, in violation of 21 U.S.C. § 846; distribution, attempted distribution and possession with intent to distribute cocaine and marijuana, in violation of 21 U.S.C. § 841(a)(1), (b)(1)(C) and (b)(1)(D), and 18 U.S.C. § 2; discharge of a firearm in connection with a drug trafficking crime, in violation of 18 U.S.C. §§ 924(c)(1)(A)(iii) and 2; murder resulting from use of a firearm during and in relation to a drug trafficking crime, in violation of 18 U.S.C. §§ 924(j)(1) and 2; witness tampering conspiracy, in violation of 18 U.S.C. § 1512(k); murder of a potential witness, in violation of 18 U.S.C. §§

1512(a) and 2; evidence tampering, in violation of 18 U.S.C. §§ 1512(b)(2)(B) and 2; witness tampering, in violation of 18 U.S.C. §§ 1512(b) and 2; Hobbs Act robbery, in violation of 18 U.S.C. §§ 1951(a) and 2; brandishing a firearm in connection with Hobbs Act robbery, in violation of 18 U.S.C. §§ 924(c)(1)(A)(ii) and 2; and illegal possession of a firearm by a convicted felon, in violation of 18 U.S.C. §§ 922(g)(1) and 924(a)(2).

3. I make this affidavit in support of two related search warrant applications that target information bearing on the presence of Burkhalter, Nesbitt and others at the scenes of offenses charged in the Second Superseding Indictment.

a. Application 22-SW-00340-LMC targets location information for Burkhalter and Nesbitt generated by a cellphone they both used accessing the Internet during the timeframe of offenses charged in the Second Superseding Indictment. To this end, the application seeks a search warrant for information associated with Joshua.Nesbitt1@gmail.com (the "Target Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant. The application seeks a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Attachment B to the proposed warrant.

b. Application 22-SW-00341-LMC targets information identifying electronic devices at the location and time of offenses charged in the Second Superseding Indictment. To this end, the application seeks a warrant to search information that is

stored at premises controlled by Google (the "Target Location Information"). The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant. The application seeks a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Section I of Attachment B to the proposed warrant. The government will then review that information and seize the information that is further described in Section II of Attachment B to the proposed warrant.

4. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A) and(c)(1)(A), because the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated," 18 U.S.C. § 2711(3)(A)(i).

5. The statements in this affidavit are based on my personal knowledge and observations, my training and experience, my review of documents, records, audio and video recordings, and information obtained from other law enforcement agents, and witnesses with direct knowledge of the facts of this case. Because this affidavit is being submitted for the limited purpose of securing the requested warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe necessary to establish probable cause in support of the requested warrant.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the statutes referred to above have been committed by Burkhalter and Nesbitt and unknown persons. There is also probable cause to search the information described in Attachment A to the proposed warrants for evidence and instrumentalities of these crimes further described in Attachment B to the proposed warrants.

GOOGLE AND RELEVANT TECHNOLOGY

7. Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

8. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet ("wi-fi") access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

9. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device's transmission range, to which it might connect.

10. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps' operation.

11. Based on my training and experience, I know Google is a company that, among other things, offers an operating system for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

12. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (e.g., Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (e.g., Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (e.g., example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

13. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited

to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

14. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

15. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. The Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

16. Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a "maps display radius," for each latitude and longitude point. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to

automatically delete their Location History and Web & App Activity after three or eighteen months.

17. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

18. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this

information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

19. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

20. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

A. The Target Account

21. The Second Superseding Indictment ("SSI") is incorporated herein by reference. The SSI charges, among the other offenses listed above, that on or about September 8, 2015, Burkhalter and Nesbitt participated in an armed robbery of a Fast Stop convenience store in Kansas City, Missouri. (D.E. 816 ¶¶ 21-22.) The SSI further charges that on or about September 10, 2015, in Raytown, Missouri, Burkhalter and Nesbitt robbed a quantity of cocaine from Danny Lamont Dean, and in the process Nesbitt shot and killed Dean with an AR-15 rifle. (D.E. 816 ¶¶ 4(b), 5-6, 9.) Soon thereafter, police learned from an individual named Anthony Dwayne Johnson that Burkhalter and Nesbitt carried out the Dean murder. Police tried to contact Burkhalter on September 14, 2015, in Kansas City but Burkhalter fled on foot before the officers could contact him. (D.E. 816 ¶¶ 4(c).) On October 2, 2015, as the SSI charges, Burkhalter fled from police again, this time by car, but was arrested after a long car chase. (D.E. 816 ¶ 4(d).) The SSI charges that two days later, on October 4, 2015, at Burkhalter's direction, Nesbitt shot and killed Johnson — the police tipster regarding the Dean murder — with the same AR-15 rifle used to kill Dean. (D.E. 816 ¶¶ 4(e), 7-8, 10-18.)

22. In connection with Burkhalter's arrest on October 2, 2015, after the car chase, police impounded the car he was driving and obtained a warrant from this Court to search the vehicle for drugs (15-SW-00303-SWH). Police seized a black LG cellphone (the "LG Cellphone") while searching the vehicle pursuant to the warrant. The Court subsequently issued a warrant to search the cellphone (20-00488-LMC). The search revealed that Nesbitt and Burkhalter both used the LG Cellphone during the month prior to its seizure, a period during which the SSI charges them with participating in the crimes described above.

23. For example, the search of the LG Cellphone revealed that "Joshua Nesbitt" was the device's owner and that the device's Bluetooth name was "Joshua Nesbitt's LGL22C." The search also connected Nesbitt to the LG Cellphone's user accounts — *e.g.*, a Snapchat account was in Nesbitt's name and a Facebook Messenger account listed the user's email as the Target Account, joshua.nesbitt1@gmail.com. The search also revealed that the LG Cellphone contained numerous "selfie"-style photographs of Nesbitt and communications with people who investigators have associated with Nesbitt, including a communication on September 2, 2015, with a relative of Nesbitt's (listed as "Cuzzzz" in the LG Cellphone's contacts), that attached a photograph of Nesbitt, Burkhalter and others. The device contained communications in which the user of the LG Cellphone self-identified as "T," which is Nesbitt's alias.

24. Burkhalter also used the LG Cellphone. Burkhalter, and not Nesbitt, occupied the car (along with another man) from which the LG Cellphone was seized after the car chase resulting in Burkhalter's arrest. Two days later, on recorded jail calls, Burkhalter described phone calls he made from the car prior to his arrest. In addition, the search of the LG Cellphone revealed electronic communications with telephone numbers and social media accounts associated with people connected to Burkhalter, including communications in which the user of the LG Cellphone self-identified as "Deuce," which is Burkhalter's alias. The LG Cellphone also accessed Burkhalter's Facebook page, bearing the username "TwoMuch Duece."

25. The search of the LG Cellphone revealed that the device ran an Android operating system and regularly accessed the Internet via Google's Chrome browser, including on September 8 and 10, 2015, respectively the dates of the Fast Stop convenience store robbery and the murder of Danny Lamont Dean. The search of the device revealed that Google location services were enabled during September 2015. The search did not reveal location information on

the device for September 8 and 10, 2015, but Google may have retained that information on its servers.

26. Based on my training and experience, I believe that users of cellphones usually carry their devices on their person when moving about the community, and that individuals engaged in drug trafficking often use and carry multiple cellphones. Moreover, in my experience, joint criminal actors — such as the SSI describes Burkhalter and Nesbitt in connection with the Fast Stop robbery and Dean murder — often carry cellphones on their person to coordinate commission of their crimes and evasion of law enforcement. For example, the Dean murder occurred during the process of a robbery of cocaine from Dean and, as the investigation revealed, Dean's cellphone was in contact immediately before the events with a phone (though not one associated with the Target Account) used at times by Burkhalter and Nesbitt, presumably to set up a meeting with Dean to transact cocaine. Likewise, with respect to the Fast Stop robbery, video surveillance footage shows that two individuals who I believe were involved in the robbery were holding cellphones by their ears while inside the establishment prior to the robbery.

27. Based on the foregoing, I believe the Target Account's Location History held on Google's servers — which as discussed above, is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device — may contain information indicating whether Nesbitt and/or Burkhalter were at or near the scene of the Fast Stop robbery and the Dean murder. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above.

28. In addition, the user's account activity, logs, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Such information can be particularly useful where, as here, a phone accessing the account has been used by more than one person, because the activity may help identify who was using the phone and when. For example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

29. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement). Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

30. I believe there is a fair probability that information concerning the Target Account, including location information, pertaining to the period between September 1, 2015, and November 5, 2015, will be relevant to the crimes charged in the SSI. This period covers the dates of the charged offenses, including time beforehand (during which preparation may have occurred) and time afterwards (during which efforts to avoid detection may have occurred). Location information throughout the period may be relevant because, when analyzed against other information uncovered by this investigation, it may help reveal or confirm the identity of

the user of the Target Account and/or the LG Cellphone at a given time and, for example, connect that person to communications revealed by the search of the LG Cellphone. In addition, the investigation has revealed that Nesbitt utilized social media accounts, including Facebook messengering services, after the LG Cellphone was seized on October 2, 2015, and prior to his arrest on or about November 5, 2015. In recorded jail telephone conversations on October 13, 14 and 17, 2015, for example, Burkhalter discussed with accomplices such ongoing communications by Nesbitt. Nesbitt's ongoing use of the Internet as a means of communications, despite the LG Cellphone's seizure, suggests that he may have accessed Google services up until the time of his arrest.

31. Therefore, with respect to the application for a warrant for information relating to the Target Account, Google's servers are likely to contain stored electronic information concerning the users of the Target Account and their use of Google services. In my training and experience, such information may constitute evidence of the crimes charged in the SSI, including information that can be used to identify the account's users, potential co-conspirators, and their whereabouts at relevant times.

B. The Target Location Information

32. The preceding section is incorporated herein by reference. The investigation determined by virtue of time-stamped video surveillance a relatively precise timeframe and location for both the robbery of the Fast Stop and the murder of Danny Lamont Dean. The Fast Stop robbery occurred on September 8, 2015, between 12:15 a.m. to 12:55 a.m., at 8431 Hickman Mills Drive, Kansas City, Jackson County, Missouri. The crime scene location, including the Fast Stop and its immediate vicinity from which the assailants launched the robbery, is a polygon defined by 38.973680, -94.549655 to 38.973890, -94.549354 to 38.973439, -94.548511, to

38.973094, -94.548961 connected by straight lines. The Dean murder occurred on September 10, 2015, at approximately 5:45 p.m. to 5:56 p.m., in the parking lot along the north side of the Mama China restaurant at 6623 Raytown Road, Raytown, Jackson County, Missouri. The relevant section of the Mama China restaurant parking lot is a polygon defined by 39.002441, -94.463568 to 39.002801, -94.463595 to 39.002784, -94.462838, to 39.002402, -94.462792 connected by straight lines. (The time/location information for these charged crimes will hereafter be referred to as the "Target Location" or, collectively, as the "Target Locations".)

33. Information regarding electronic devices at the Target Locations, and the user(s) of such device(s), may constitute evidence of the crimes charged in the SSI, including the Fast Stop Robbery and Dean murder. Presence of the LG Cellphone at the Target Locations may indicate that Nesbitt and/or Burkhalter were present at the Target Locations (to the extent that information is not among location information associated with the Target Account, as discussed above). The presence of other devices at the Target Locations may indicate other individuals' presence at the Target Locations. Such information may constitute evidence of the charged criminal activity and/or be helpful in identifying potential witnesses with relevant information.

34. Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Locations for evidence of the crime(s) under investigation. The information to be searched includes (1) identifiers of each device; (2) the location(s) reported by each device to Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

35. The proposed warrant for Target Location Information sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as

described in Section I of Attachment B to the warrant:

a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Locations. For each device, Google will provide a anonymized identifier, known as a Reverse Location Obfuscation Identifier ("RLOI"), that Google creates and assigns to device for purposes of responding to this search warrant; Google will also provide each device's location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e.*, "maps display radius"), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.*, example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.

b. The government will identify to Google the devices appearing on the list produced in step 1 for which it seeks the Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

c. Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

36. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed

to the government.

CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrants. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Det.

Leland W. Blank, Detective
Kansas City, Missouri Police Department

Sworn and attested by affiant via telephone, after being submitted to me by reliable electronic means on this 7th day of June, 2022. Sworn to by telephone 11:20 AM, Jun 7, 2022

Lajuana M. Counts

Honorable Lajuana M. Counts
United States Magistrate Judge
Western District of Missouri